




Workbooks.com

GDPR:  
*5 Steps  
Checklist*



The General Data Protection Regulation (GDPR) is a new legal framework that comes into force on May 25th 2018. It builds upon the existing Data Protection Act. GDPR will significantly impact businesses with many having to change their current data protection practices and policies to ensure compliance.

Please note: The Data Protection Bill is currently going through UK Parliament, which will enforce the EU's GDPR standards, preparing Britain for Brexit. The main elements of the bill include implementing GDPR standards across all general data processing and providing clarity on the definition used in the GDPR in the UK context. You can find out more information from this [Data Protection Bill Factsheet](#) and the [ICO website](#).

GDPR is about creating a higher global standard for data protection, privacy and security. GDPR has transparency and accountability at its heart. It is about business continuity and mitigating risks.

## THE GENERAL THEMES OF GDPR ARE:

- Improve the protection of an individual's personal data
- Harmonise the laws across the EU
- Strengthen the legislation imposing more obligations on 'Data Processors', not just 'Data Controllers'

GDPR is complex, it contains 173 recitals and 99 articles. If you want to dive into the depth of GDPR, we suggest you go to the [European Commission's website](#).

To help decipher the main things you should consider as part of your GDPR preparation, we have compiled a 5 steps checklist.

1

# *Increase awareness within your business...*

## **AND MAKE IT A PRIORITY, NOW!**

If you haven't already, raise the awareness of the importance of GDPR compliance with all key stakeholders in your organisation. They need to appreciate the impact GDPR is likely to have and help you to identify the areas that could cause compliance problems. This will help create your priority list and help you define your plan of action in order to be compliant by the deadline of May 25th 2018. Make no mistake: GDPR is truly a top management discussion. The impact of non-compliance can be substantial i.e. 4% of global turnover or £20m, whichever is higher... And that is before you take into consideration the reputation damage incurring such a fine would bring too.

**Keep in mind that implementing GDPR could have significant resource implications for your business.**

Define a project team, with key champions within each department. But above all else, don't delay or you may find compliance difficult if you leave your preparations to the last minute.

2

# *Assess your organisation*

## **AND AUDIT THE INFORMATION YOU HOLD**

The first thing you need to do with GDPR is to review existing privacy and security procedures and set-up in order to identify your business strengths and weaknesses. You need to clearly identify all the systems (electronic and paper) where you store personal data and do an audit of all the data you currently hold, whether it is prospects, customers, suppliers, partners, employees etc. No stone should be left unturned.

You should also review all your data processing activities, for example: how do you create a new contact in your CRM, how do you process employees information during on-boarding and throughout their employment, how do you manage CVs from candidates, how do you record suppliers information etc.

Document the personal data you hold, the source of such data and details of with whom you share this data. Review all your document processes and identify what needs to be changed in order to ensure compliance going forward. Don't forget information that may also be attached to email e.g. CV's during your recruitment processes. Consider how you can change your processes to store this information in one central place rather than email.

**In summary, conduct a data audit and data mapping to fully understand what data you have and how you are going to lawfully process it going forward.**



# 3

## Define the lawful grounds

### FOR PROCESSING PERSONAL DATA

GDPR requires that you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful ground under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful ground applies. If no lawful basis applies to your processing, your processing will be unlawful.

The individual's right to be informed under Article 13 and 14 requires you to provide people with information about your lawful grounds for processing. This means you need to include these details in your privacy notices whenever data is being collected and processed.

**So once you have done your data audit, you need to identify on what lawful ground you can process data. You must have a valid lawful basis in order to process personal data.**

The lawful grounds for processing set out in Article 6 of GDPR are:

- 1. Consent:** the individual has given clear consent for you to process their personal data for one or more specific purposes.
- 2. Contract:** the processing is necessary for a contract to which the individual is party, or because they have asked you to take specific steps before entering into a contract.
- 3. Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- 4. Vital interests:** the processing is necessary to protect the vital interests of the data subject or of another natural person.
- 5. Public interest:** the processing is necessary for you to perform a task in the public interest or in the exercise of official authority vested in the controller.
- 6. Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests, in particular where the data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks).

Several of the lawful grounds relate to a specific purpose – a legal obligation or a contract with an individual etc. If you cannot identify and justify a lawful ground for some of the data that you currently hold, this particular data should be deleted. When reviewing the lawful ground for processing, you should always consider the purpose for which you are processing data and the nature of your relationship with the individual.

It's important to get this right first time. According to the ICO, 'If you find at a later date that your chosen basis was actually inappropriate, you cannot simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.'





# 4

## Establish control, REVIEW PROCEDURES AND PROCESSES

With GDPR, individuals will have enhanced rights to access their information, have any inaccuracies corrected, have information erased, data portability etc.

You need to review privacy/data protection procedures and policies to ensure that they provide for each enhanced right under GDPR.

**Privacy information:** With GDPR, additional information must be given to individuals when their personal data is obtained. Ensure privacy notices are available wherever personal data is collected, on your website for example. Under the transparency provisions of the GDPR, the information you need to give people included your intended purposes for processing the personal data; and the lawful basis for the processing. This applies whether you collect the personal data directly from the individual or you collect their data from another source. You can find out more on the [ICO website](#).

**Individual rights & Subject Access Requests:** Current rules for subject access requests are changing: timescales for compliance will be reduced, fees will generally no longer be chargeable and additional information will be required to be provided to individuals e.g. data retention periods and the right to have inaccuracies corrected. You'll need to establish robust procedures to respond to data subject requests for access, rectification, objections, restriction, portability and deletion (right to be forgotten).

**Data breaches:** GDPR widens the number of businesses obliged to notify the ICO and private individuals of data breaches. Failure to comply with this obligation may lead to significant fines by the ICO. You'll need to review and adjust administrative, physical and technological security measures and processes to detect and respond to security breaches. Ensure that there are procedures in place to detect, investigate and report on personal data breaches. The ICO suggests assessing the types of data held and documenting which ones would trigger notification in the event of a breach.

Other areas you should consider includes:

- Establish a privacy impact assessments process.
- Review contracts with your suppliers and affiliates that may be processing data on your behalf.
- Create a mechanism to manage data subject preferences.
- Implement controls to limit the organisations use of data to the purposes for which it collected the data. The more you can automate, the better.
- Train all employees on procedures and process changes. Drive security and privacy awareness session etc.
- Determine whether you need to appoint a Data Protection Officer, and if you determine you are not required to, then make sure that decision is documented.



# 5

## Document COMPLIANCE

Under the accountability principle, you are expected to be able to demonstrate that you are complying with GDPR, and that you have appropriate policies and processes in place. You need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You therefore need to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. You may also want to record a proof of the lawful ground, like consent for example. CRM can play a vital part in recording that information and tracking compliance over time. This is something that could become a real challenge if you are managing your data in excel spreadsheets for example.

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data. You will also in most cases need to gain explicit consent from the data subject to the processing. You can find out more information on the [ICO website](#).

Keep a copy of all your privacy notices and consent forms, data inventory. Document all data processing activities. Ensure policies, procedures and processes are documented and update as changes are made.

## CONCLUSION

We hope this short checklist will help you focus your time between now and May 25th to ensure you are ready for GDPR.

For additional guidance, we suggest you go to the [ICO website](#), in particular to their [12 steps to take to prepare for GDPR](#).

